SHASTA CLOUD

HOW-TO GUIDE

Admin Identity Management

Inviting, editing, and managing admin identities in Shasta Cloud

DOCUMENT TYPE

How-To Guide

PLATFORM

Shasta Cloud v4.1

LAST UPDATED

April 23, 2026

VERSION

1.0

Contents

Table of Contents

Overview

This guide covers how to manage admin identities in Shasta Cloud — inviting new users, editing organization settings, enabling multi-factor authentication, and editing, resending, or deleting existing identities. All tasks use Shasta Cloud's role-based access control model with **Base Roles** and **Add-On Roles**.

Prerequisites: You must be signed in to Shasta Cloud as an admin-role user and (where noted) navigated to the appropriate Org or MSP.

Scope: Admin Settings | Requires: Admin Role | RBAC: Base + Add-On | Shasta Cloud Platform

Step 1 — Invite a New Identity for MSP

Navigate to: `Admin → Settings`

In the left navigation panel, click **Admin** to expand it, then click **Settings**. This opens the `Admin / Settings` page with two tabs: **Overview** and **Security**.

Click the **Security** tab. The Security page contains two sections:

- **Authentication** — with the organization-level MFA toggle
- **Identities** — a list of all configured identities, with an **Invite** button in the top-right

If no identities have been configured, the list will be empty. Click the **Invite** button to open the Invite Identity form.

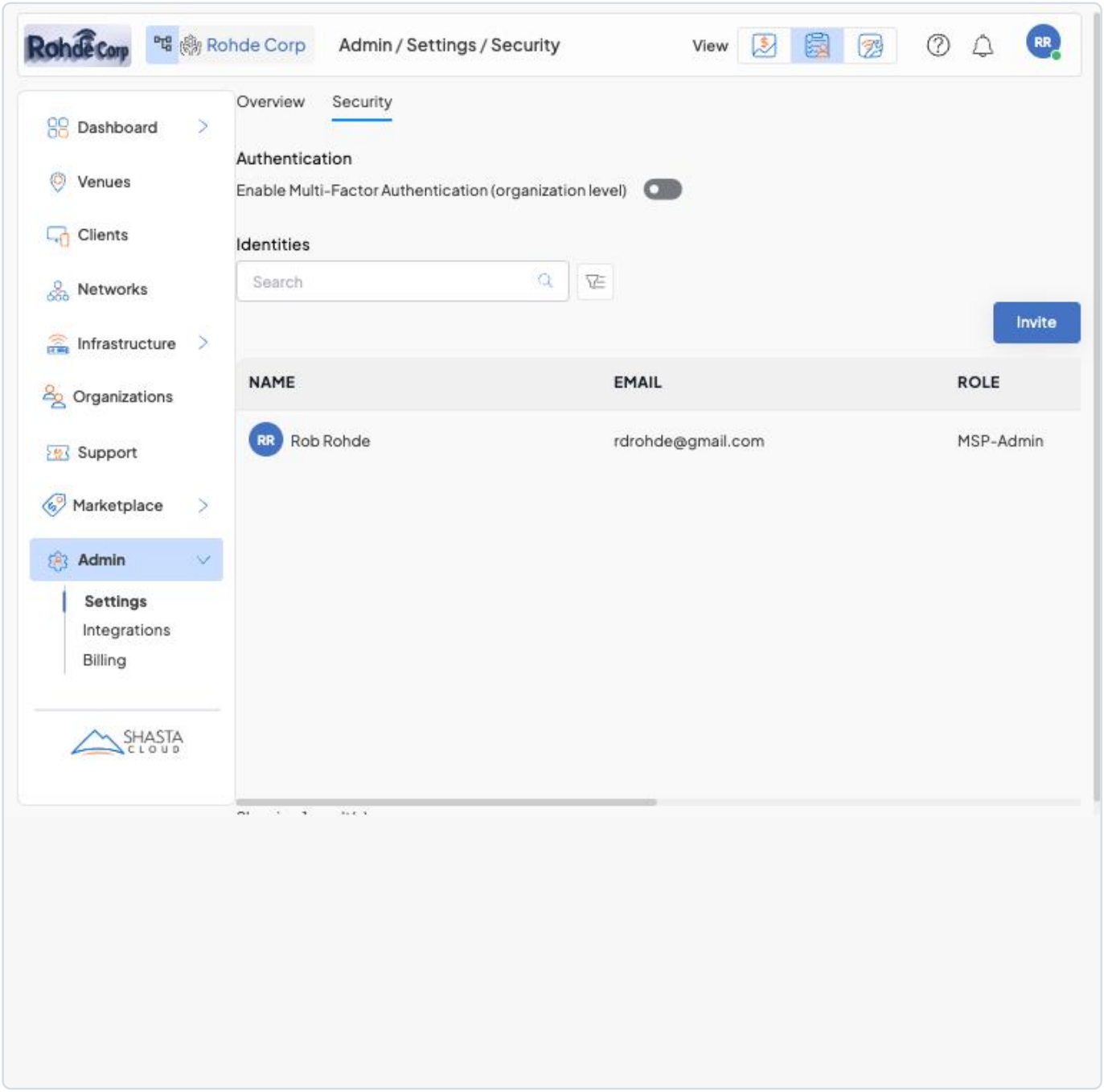

Figure 1 — Admin → Settings → Security tab showing the Authentication section (MFA toggle) and the Identities section with an Invite button.

The Identities table includes these columns (scroll right to see them all):

Column	Description
Name	Name and initials of the identity.
Email	Email address of the configured identity.
Role	List of roles the identity is granted.
Last Accessed	Last login timestamp (timezone-aware).
Enable	Toggle to enable or disable access without removing the identity.
Actions (⋮)	Row action menu for Edit, Resend, or Delete operations.

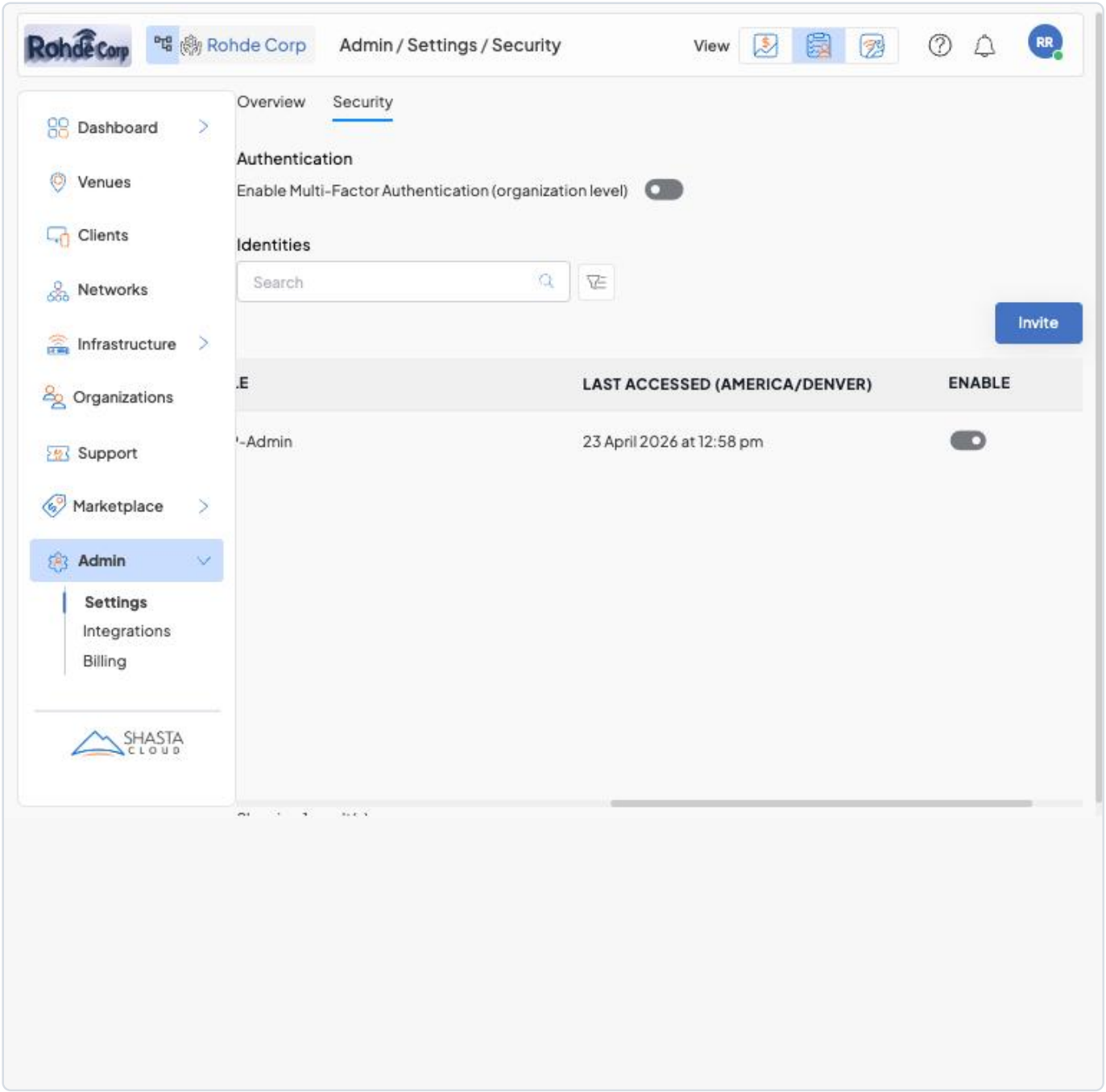

Figure 2 — Scroll right on the Identities table to reveal the Last Accessed and Enable columns.

Fill in the Invite Identity form

On the Invite Identity page, complete all required fields:

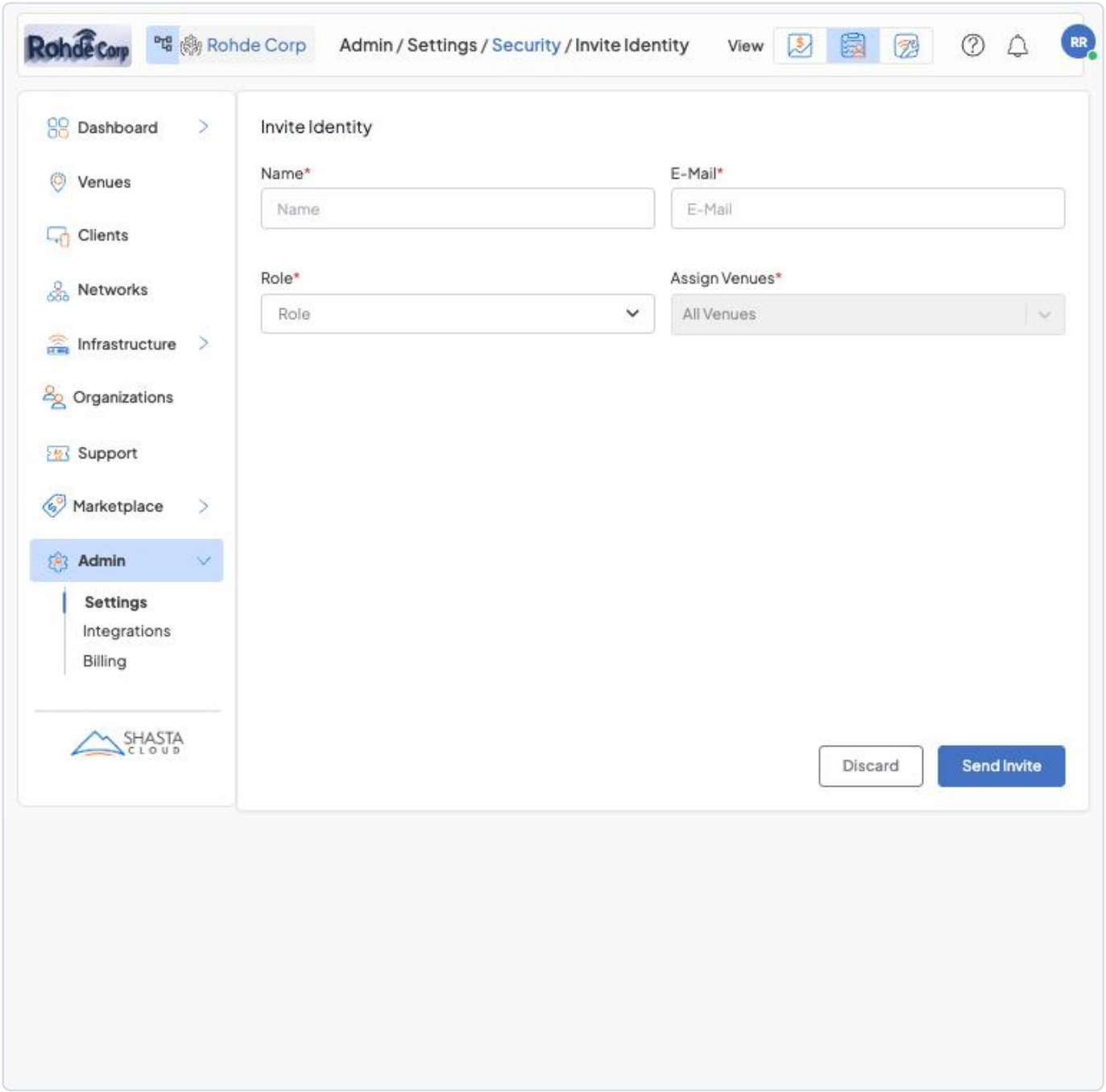

Figure 3 — The Invite Identity form with Name, E-Mail, Role, and Assign Venues fields.

Field	Type	Required	Notes
Name	Alphanumeric	**Required**	Up to 30 characters.

Field	Type	Required	Notes
E-Mail	Email format	Required	Standard email address.
Role	Dropdown	Required	Select one or more roles (see Step 2).
Assign Venues	Dropdown	Required	Defaults to "All Venues".

Click **Send Invite** to complete the invitation. The invited identity appears in the Identities list:

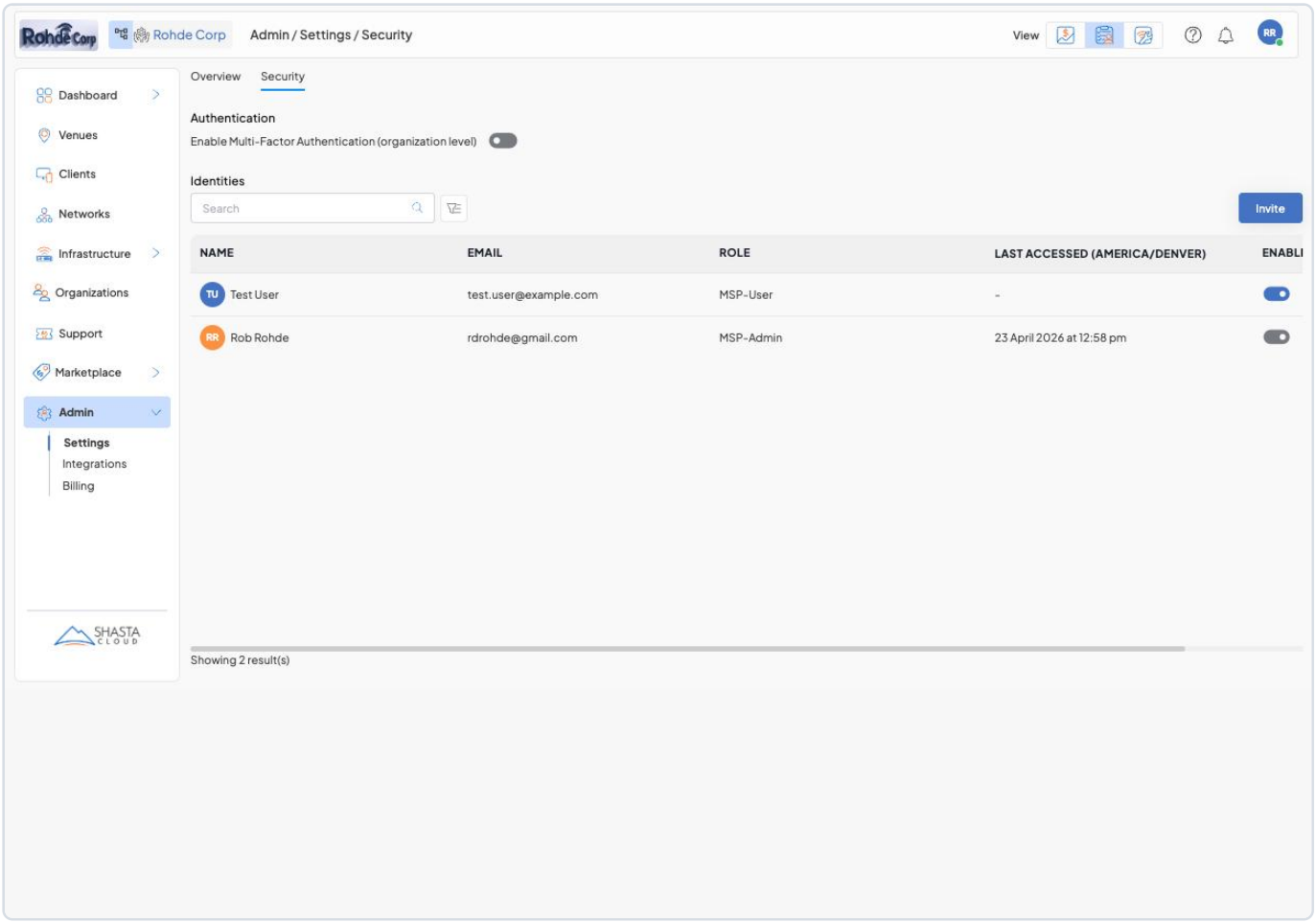

Figure 4 — Identities list after inviting a new user. "Test User" appears with role MSP-User. The Enable toggle is on by default and Last Accessed is blank until first login.

> **Tip:** The Enable toggle lets you temporarily disable an identity without deleting it — useful for contractors, seasonal staff, or suspending access during an investigation. Toggling it back on restores full access immediately, with no need to re-invite.

Step 2 — Understanding Roles: Base Roles & Add-On Roles

When you click the **Role** dropdown in the Invite Identity form, roles are organized into two categories:

- **Base Roles** — the primary access tier for the user
- **Add On Roles** — supplemental permissions that can be combined with a Base Role

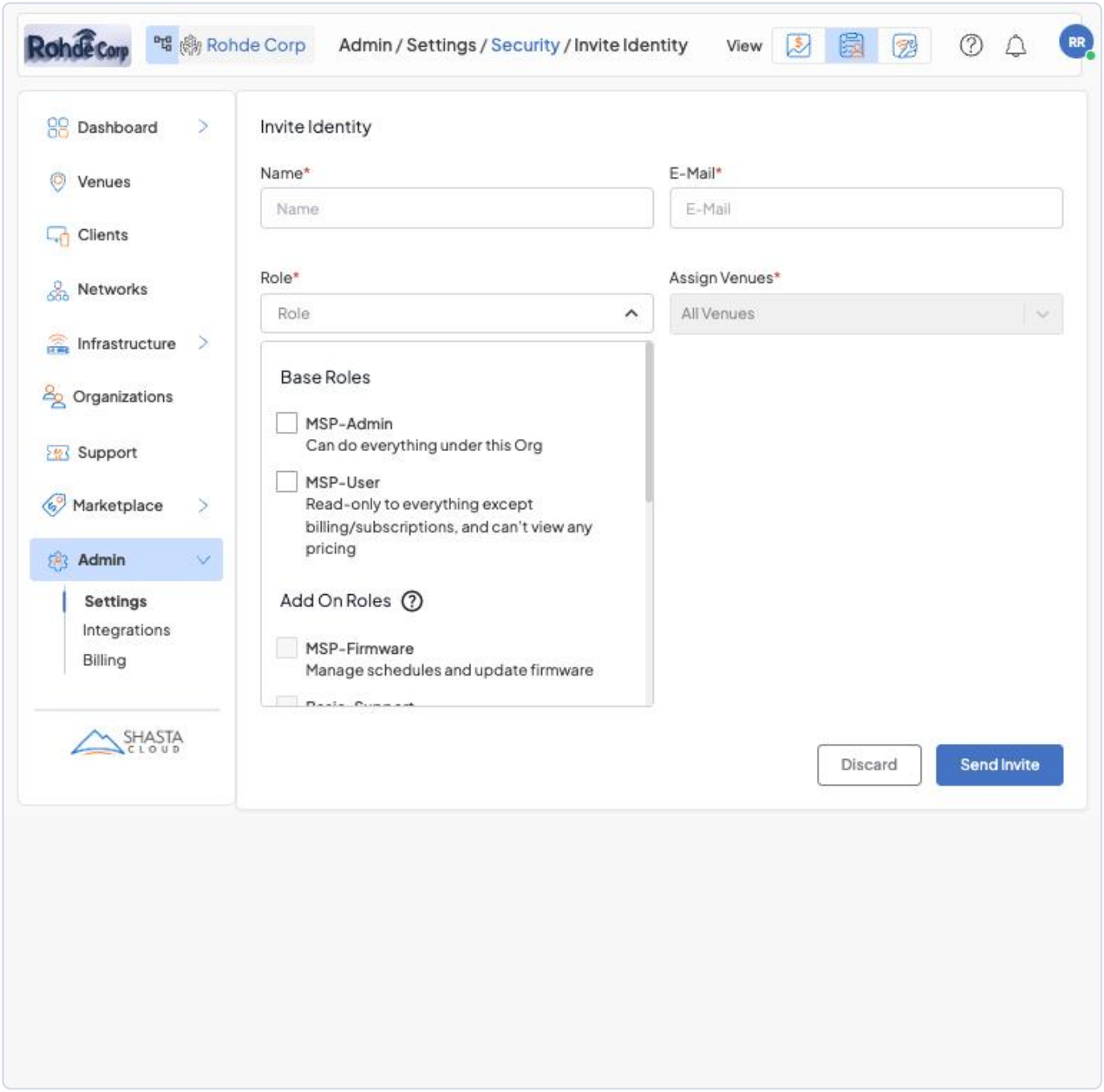

Figure 5 — Role dropdown showing Base Roles (MSP-Admin, MSP-User) at the top and the beginning of the Add-On Roles list below.

Base Roles

Role	Access Rights
MSP-Admin	Can do everything under this Org.
MSP-User	Read-only access to everything except billing/subscriptions, and cannot view any pricing.

Scroll down in the Role dropdown to see the full list of Add-On Roles:

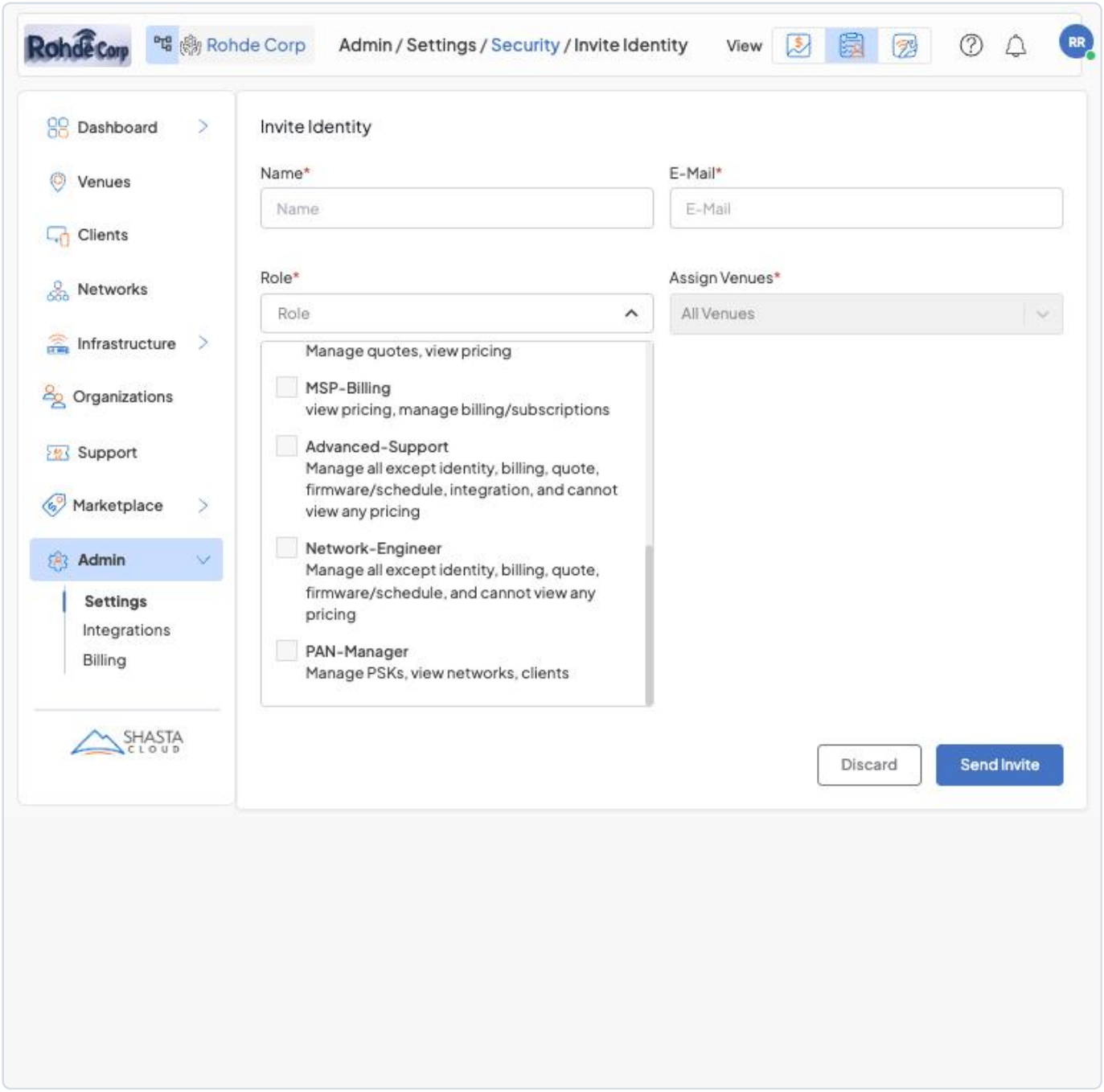

Figure 6 — Role dropdown scrolled down to show the full list of Add-On Roles: MSP-Business, MSP-Billing, Advanced-Support, Network-Engineer, and PAN-Manager.

Add-On Roles

Role	Access Rights
MSP-Firmware	Manage schedules and update firmware.
Basic-Support	Perform infrastructure reboot, factory reset, and troubleshooting tools.
MSP-Business	Manage quotes, view pricing.
MSP-Billing	View pricing, manage billing/subscriptions.
Advanced-Support	Manage all except identity, billing, quote, firmware/schedule, integration; cannot view pricing.
Network-Engineer	Manage all except identity, billing, quote, firmware/schedule; cannot view pricing.
PAN-Manager	Manage PSKs; view networks and clients.

Combining roles: A user can have one Base Role plus any number of Add-On Roles. For example, an **MSP-User** with the **Basic-Support** add-on can read everything across the Org and also perform reboots and factory resets — but still cannot modify configuration or view pricing.

Step 3 — Edit Organization Settings

Prerequisites: Admin-role user, logged into Shasta Cloud, and navigated to the appropriate Org.

Navigate to: `Admin → Settings → Overview tab`

On the Overview tab, you can configure or modify the organization's core information — name, address, logo, organization type, and notes.

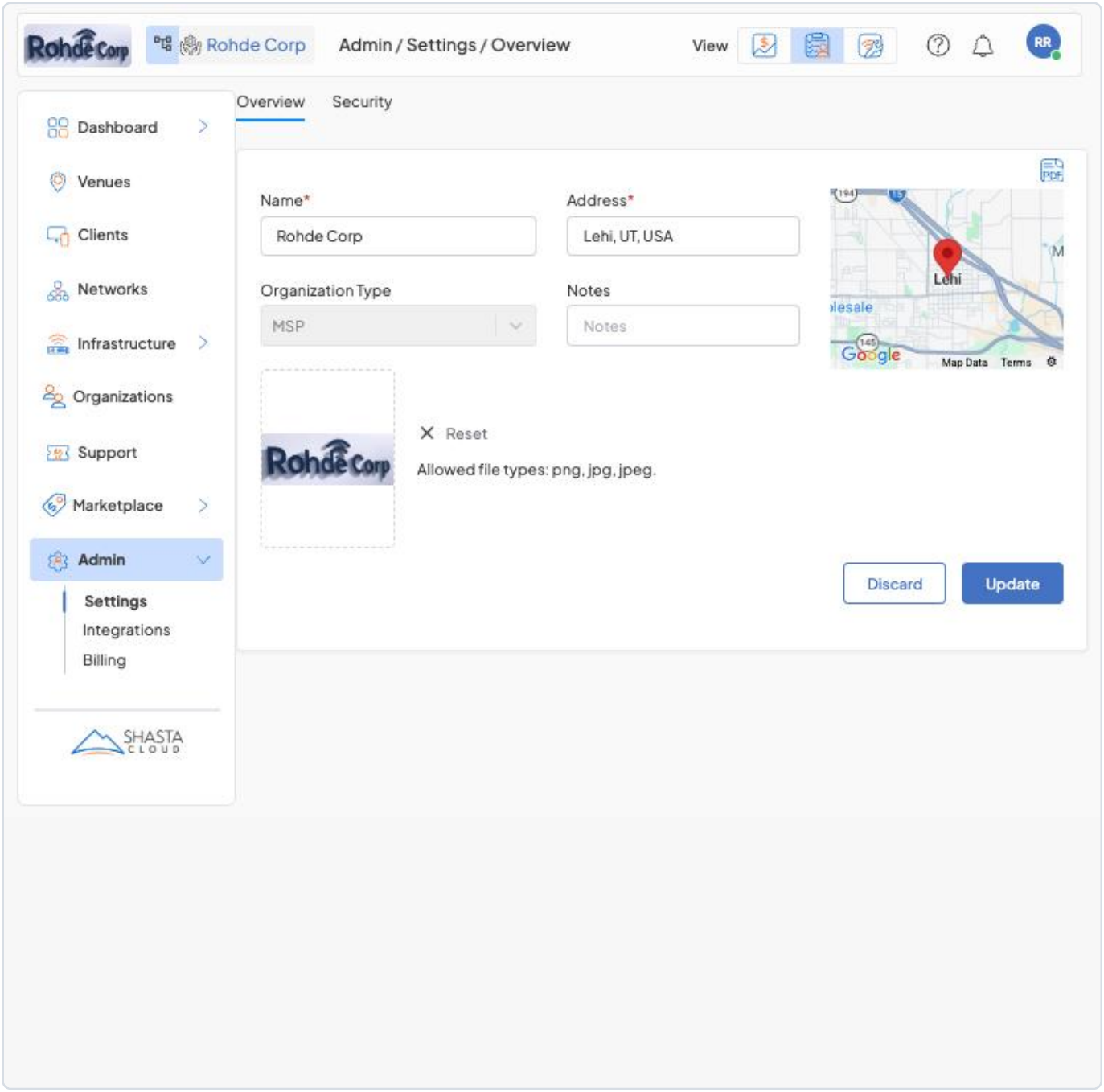

Figure 7 — Admin Settings Overview tab showing Name, Address (with Google Maps preview), Organization Type, Notes, the logo upload area, and the Discard / Update buttons.

Field	Type	Required	Notes
Name	Alphanumeric	**Required**	3 to 45 characters.

Field	Type	Required	Notes
Address	Alphanumeric	Required	Up to 250 characters. Auto-suggests Google Maps addresses as you type.
Organization Type	Dropdown	Optional	Displays the org type (e.g., MSP).
Notes	Alphanumeric	Optional	Up to 320 characters.
Logo	Image upload	Optional	Allowed file types: PNG, JPG, JPEG.

> **Note:** When typing in the **Address** field, the text box suggests matching Google Maps addresses. Choose a suggestion to auto-fill the mini-map preview, or continue typing a custom address.

Click **Update** to save changes, or **Discard** to cancel.

Step 4 — Enable Multi-Factor Authentication (MFA)

Navigate to: `Admin → Settings → Security tab`

The Security page's **Authentication** section contains the **Enable Multi-Factor Authentication (organization level)** toggle. When enabled, all users in the organization will be required to set up MFA on their next login.

Click the toggle to enable MFA. A confirmation dialog appears — click **Yes** to confirm. After a brief moment, the operation completes and MFA is enabled for the organization.

> **Important:** To disable MFA at any time, click the toggle again and confirm the dialog. Users who already enrolled in MFA will keep their authenticator registration; disabling at the org level simply stops requiring it at login.

Step 5 — Edit an Identity

Prerequisites: Admin-role user, logged into the appropriate Org or MSP.

Navigate to: `Admin → Settings → Security tab`

On the identity row you want to modify, scroll the table to the right to reveal the ⋮ Actions column.

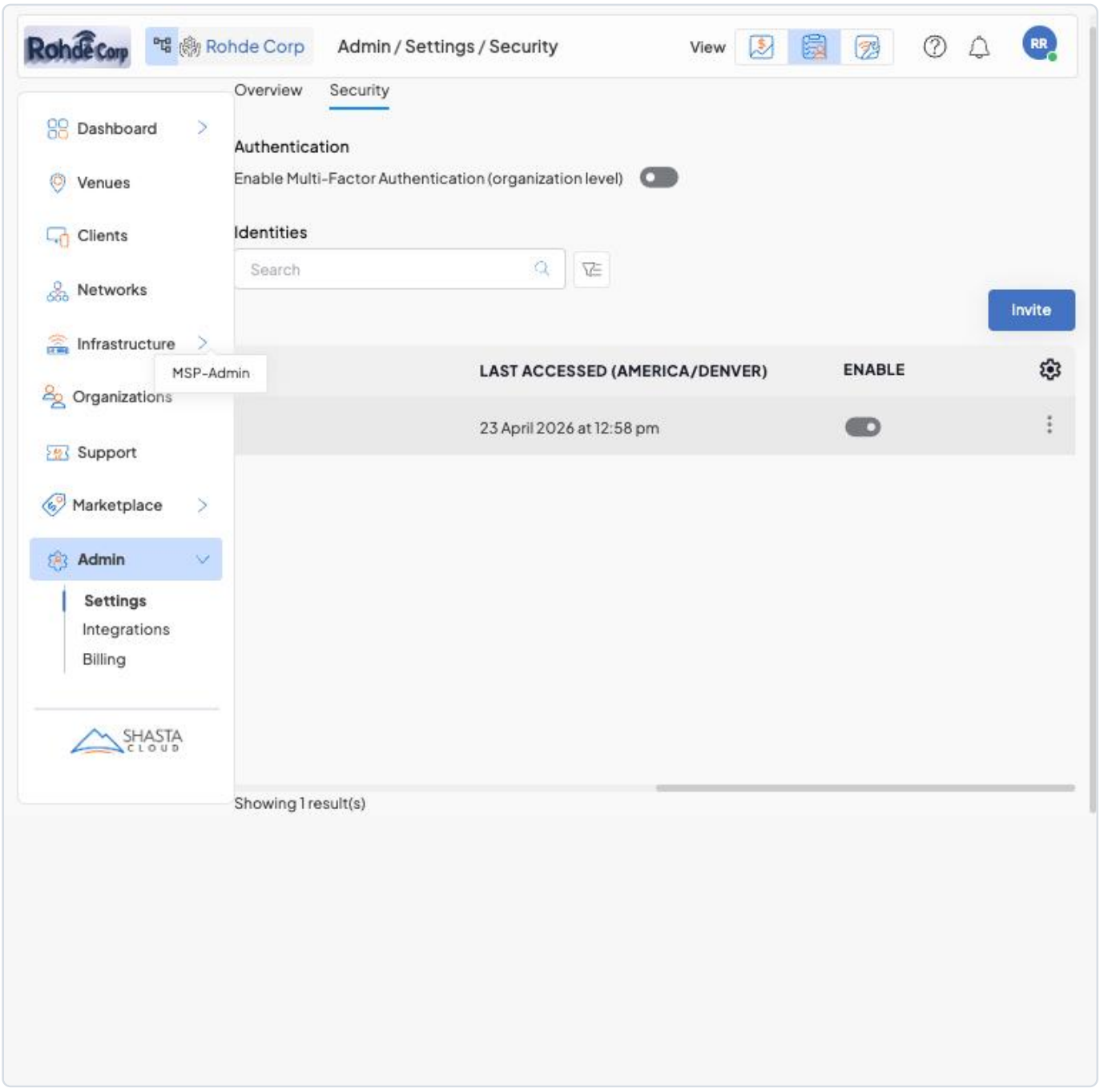

Figure 8 — Scroll the Identities table to the right to reveal the Enable toggle and the ⋮ Actions menu for each identity.

Click the ⋮ icon on the identity row, then choose **Edit**:

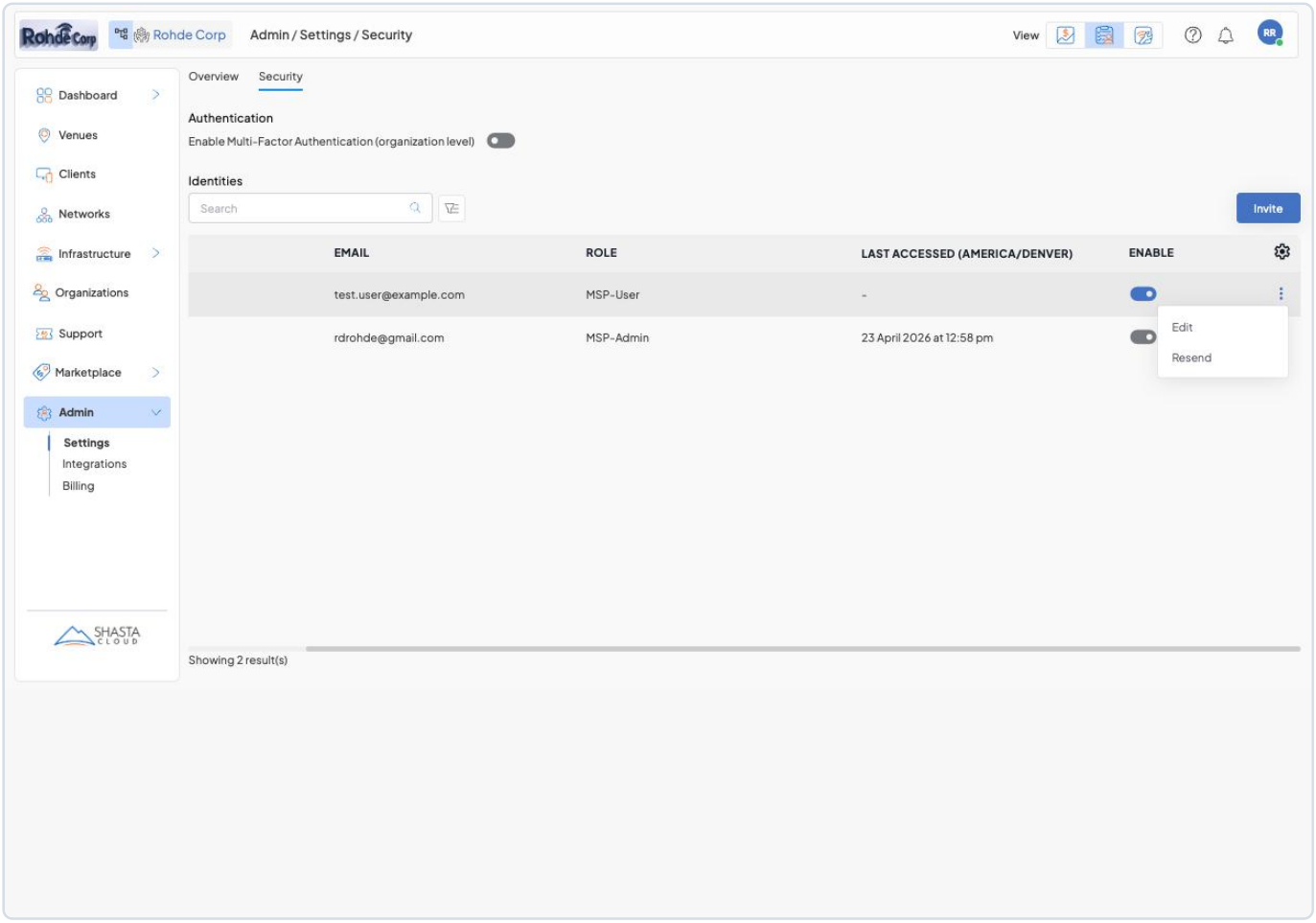

Figure 9 — The ⋮ Actions menu open on the Test User row, showing Edit and Resend options.

The **Edit Identity** form opens. Modify the Name, E-Mail, Role, Phone, or Assigned Venues as needed:

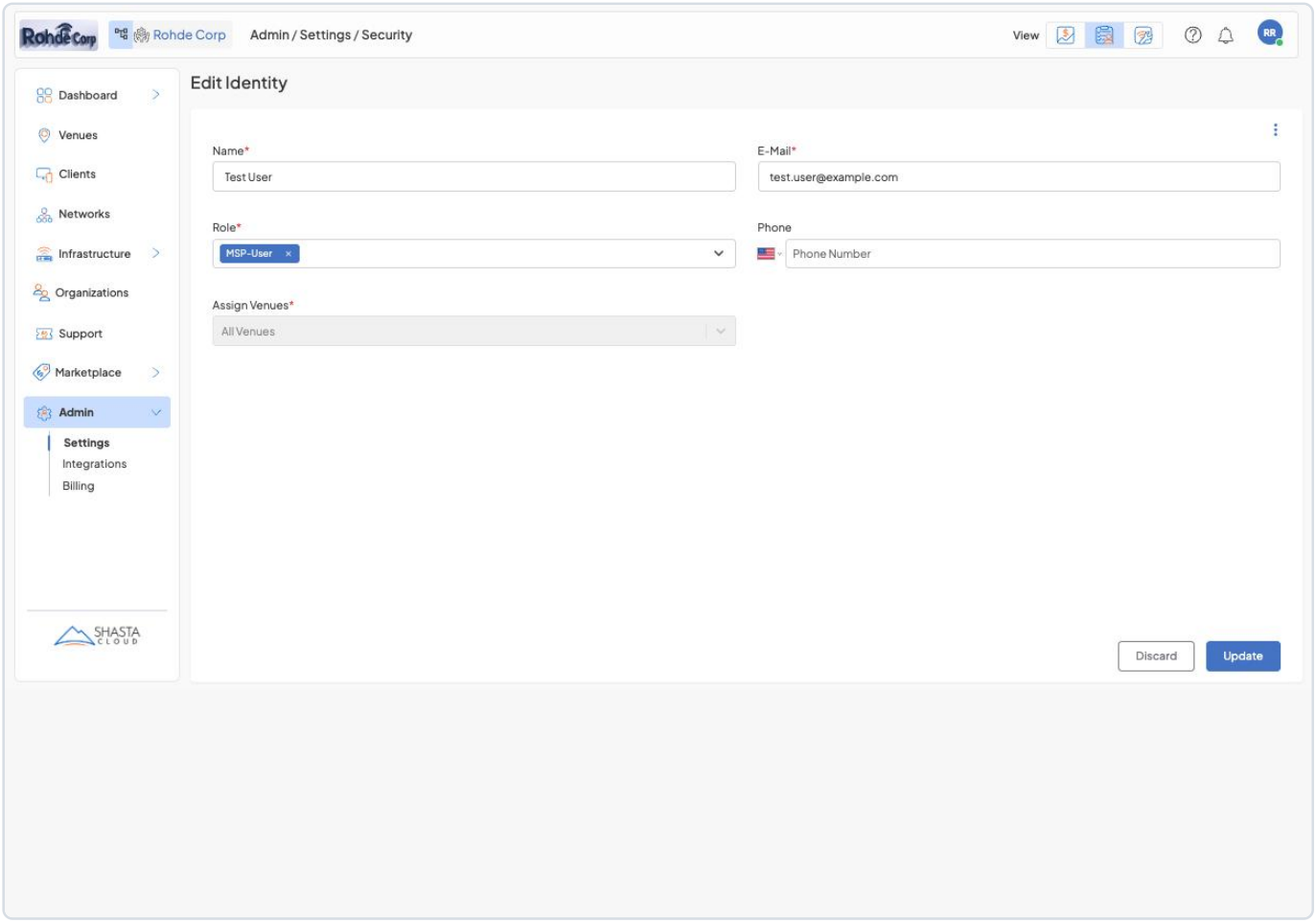

Figure 10 — The Edit Identity form. The Role field shows the currently-assigned roles as removable chips (e.g., MSP-User). Phone is available but optional.

Click **Update** to save changes, or **Discard** to cancel.

> **Tip:** Removing a role chip from the **Role** field immediately stages that change; it only takes effect when you click **Update**. Use this to safely preview a permission change before committing.

Step 6 — Resend an Invite

If an invited user never received or acted on their invitation email, you can resend it without creating a new identity.

Navigate to: `Admin → Settings → Security tab`

1. Locate the identity in the list and scroll right to reveal the ⋮ icon.

2. Click ⋮ and choose **Resend** (shown in Figure 9 above).
3. A confirmation banner appears indicating the invite has been resent.

> **Note:** Resend generates a fresh invitation link. Any previous invite link for that identity is invalidated — the user must use the most recent email.

Step 7 — Delete an Identity

Deleting an identity is done from the **Edit Identity** page rather than the Identities list.

Navigate to: `Admin → Settings → Security → ⋮ → Edit`

On the Edit Identity page, click the ⋮ icon in the top-right corner of the form. A small menu appears with a **Delete** option:

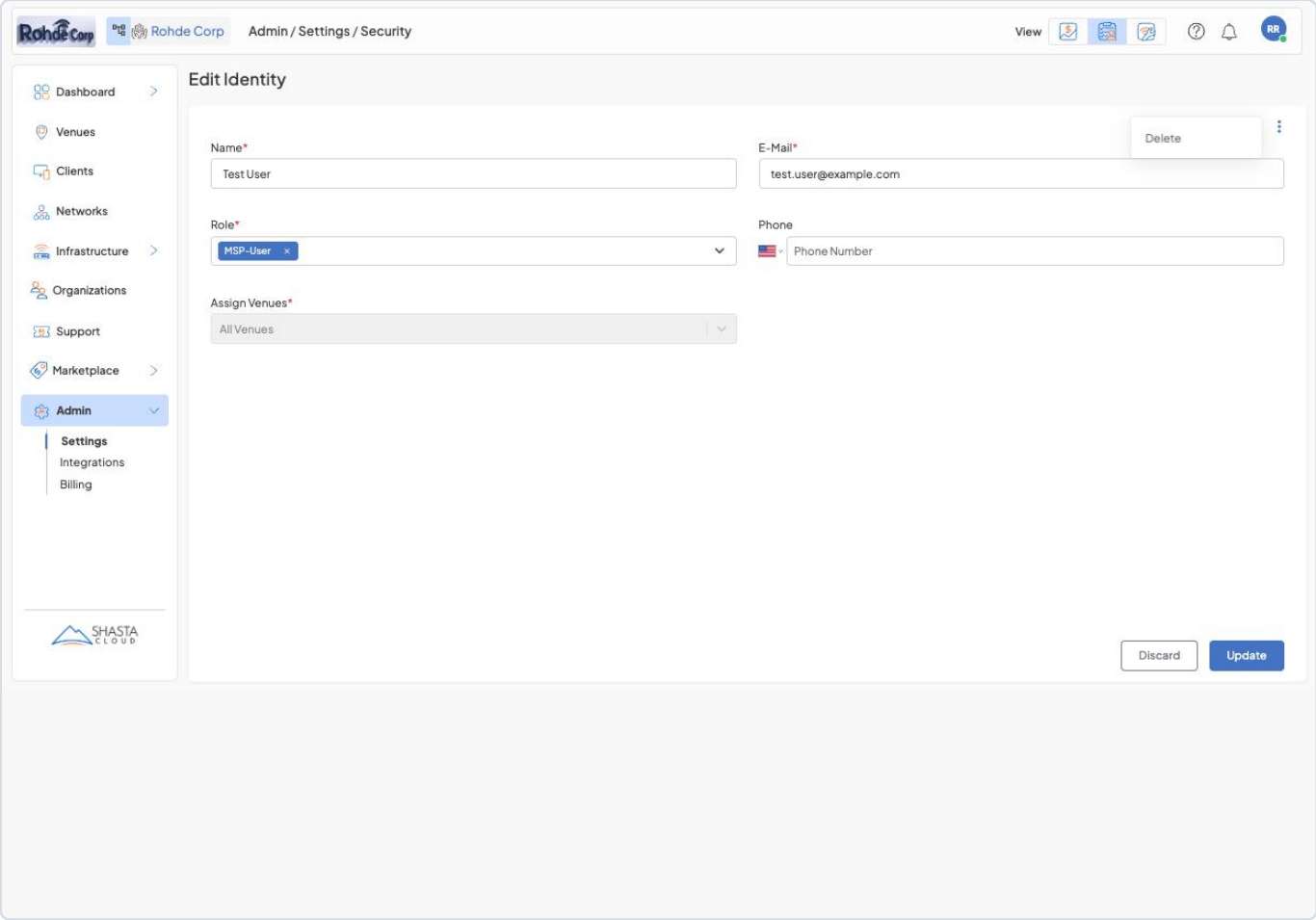

Figure 11 — The Edit Identity page with the ⋮ menu open, revealing the Delete action. Click Delete and confirm the dialog to permanently remove the identity.

> **Warning:** Deletion is permanent. The identity is removed from the organization and any active sessions are invalidated. If you only need to temporarily block access, use the **Enable** toggle on the Identities list instead (Step 1, Figure 2).

For further assistance, please reach out to Shasta Cloud support.